Instruction Slides for #33 Supply Chain Risk Management

Assembled from public presentations prepared and delivered by Subject Matter Experts Carol Woody, Ph.D. and Robert Ellison, Ph.D.

© 2014 Carnegie Mellon University

Copyright 2014 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM-0001959

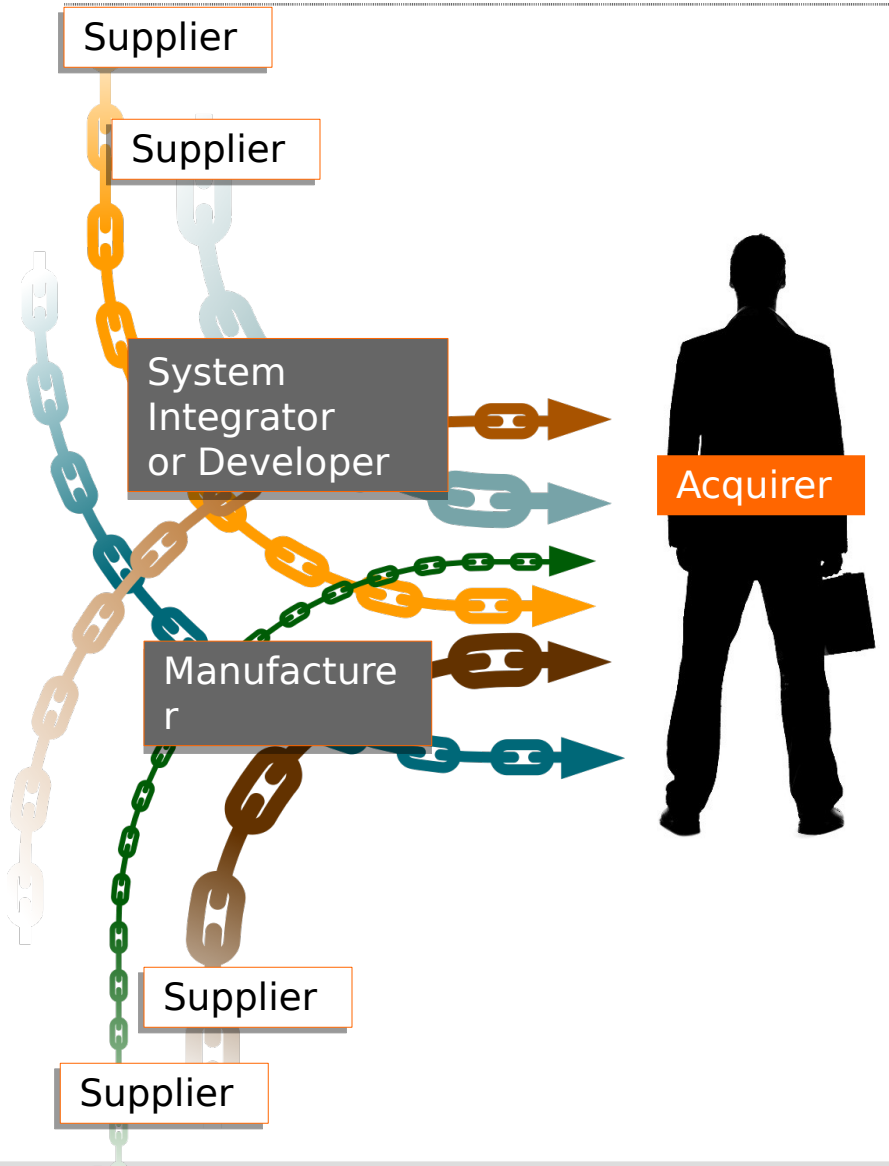
Slide Notes

The notes for some slides include the content from the script used in a video.

ELO 33.1.1

Understand the supply chain risks that affect the DoD and how are they exhibited in hardware and software supply chains (tainted products, counterfeits, malware, vulnerabilities, etc.)

General Supply Chain Problems



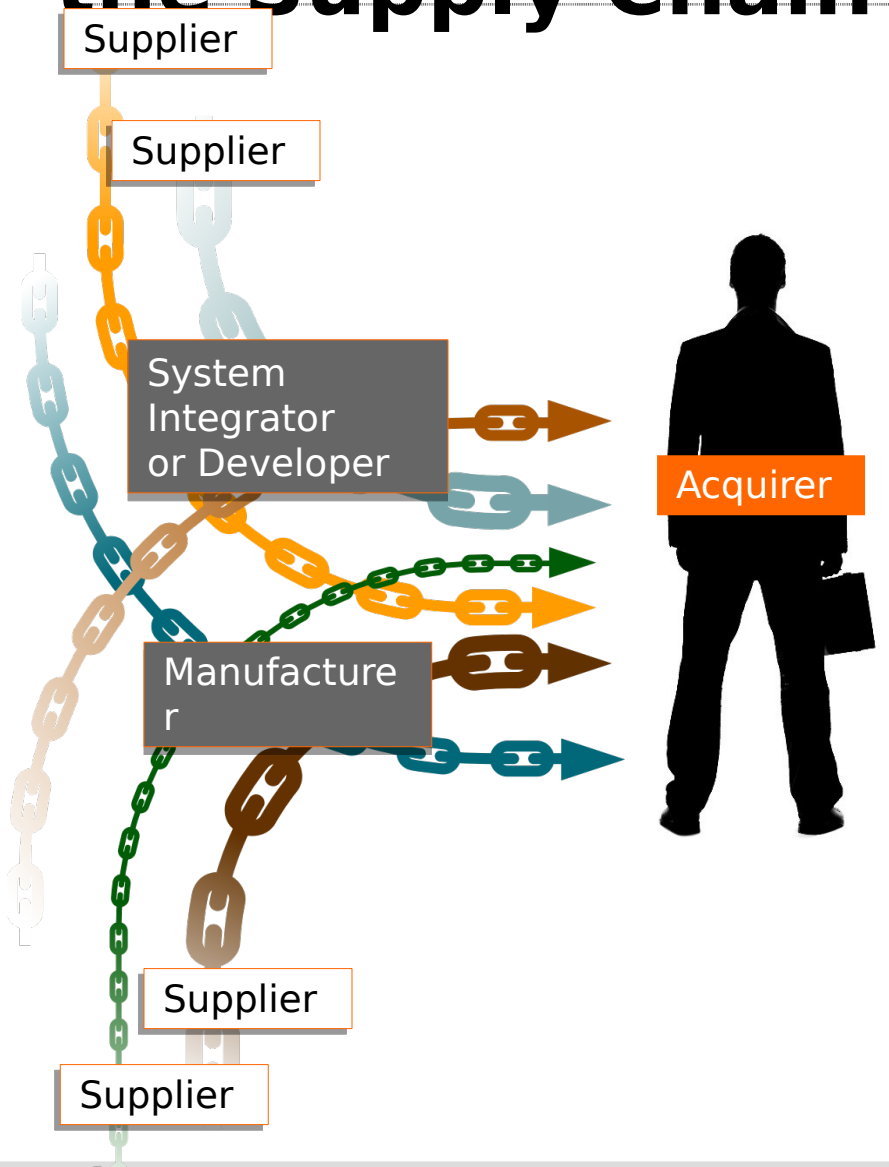
Long supply chains

- many organizations
- many countries
- many products and subcomponents
- opportunities for good and bad things to happen

Marketplace

- products are valued for features.
- acquirers don't value secure products.
- suppliers are not rewarded for secure products.
- product integrity is not valued.

Problems Occurring through and to the Supply Chain



Supply chain compromised : weakness intentionally inserted

- consequences include counterfeit and malware insertion
- resulting from poor supply chain management and and supplier selection

Authentic system compromised: weakness unintentionally created

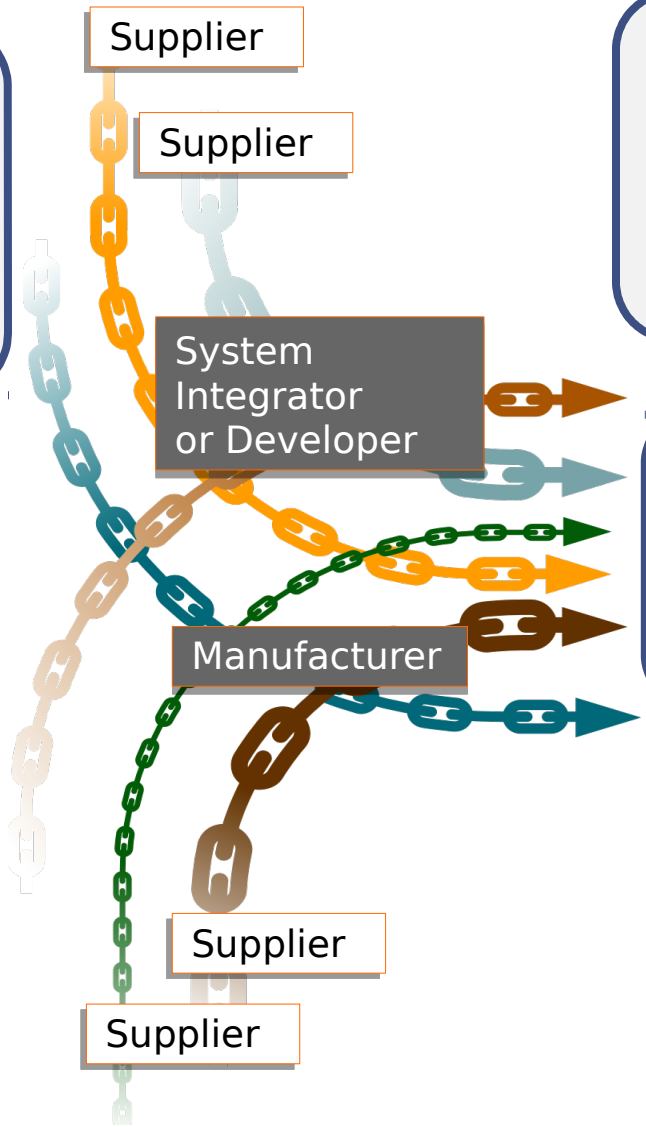
- consequences include information disclosure and data tampering
- many resulting from poor development practices, supplier selection.

Result: Systems with adverse behaviors

Supply Chain Risks

Compromises supply chain logistics
- inserts counterfeits components
- inserts malicious software (malware)

Poorly secured supply chain and untrusted suppliers



Compromises authentic & deployed system
- disclosures information
- tampers with data

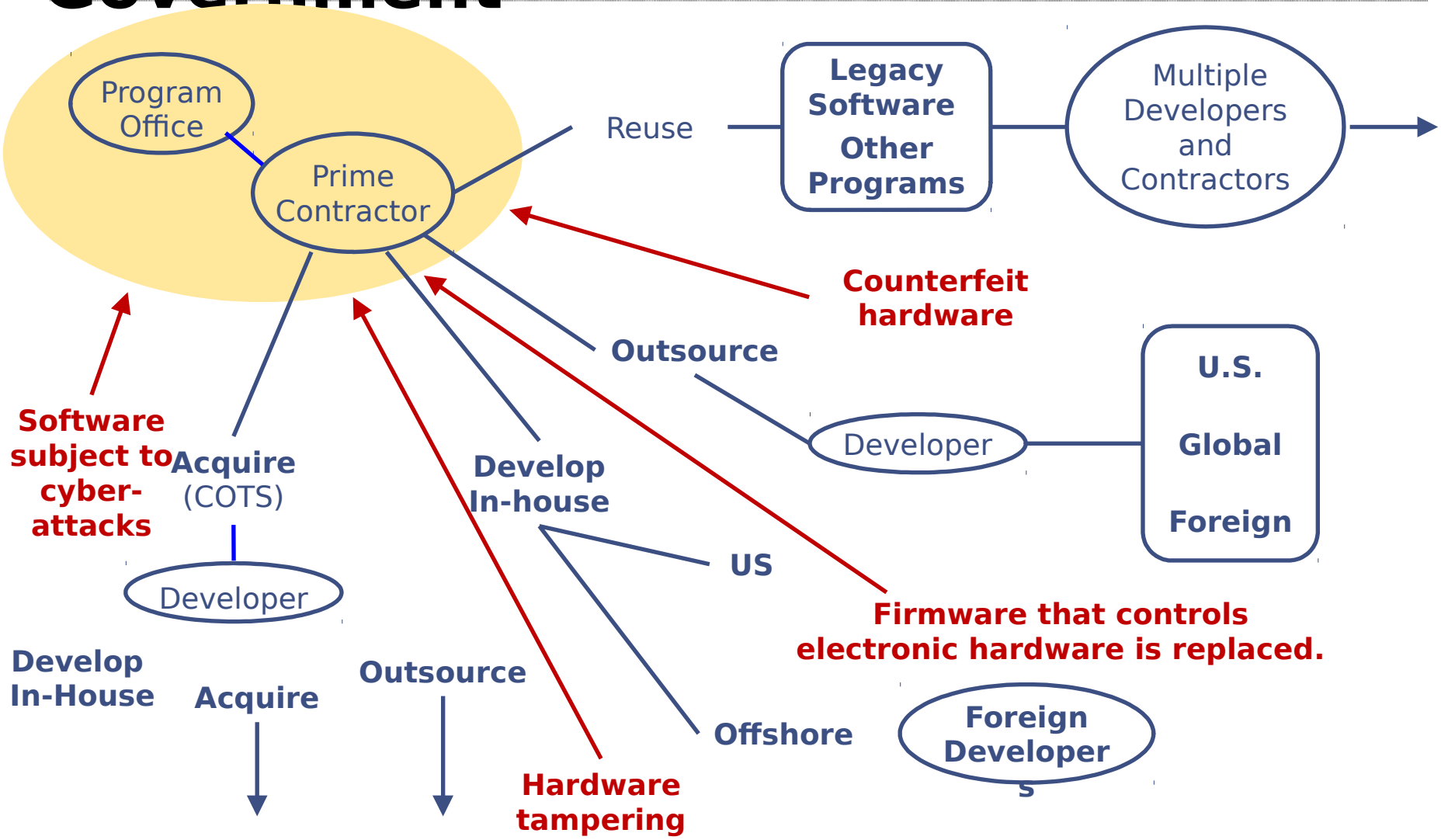
System weaknesses unintentionally created during development

Government System Supply Chains

Items of interest include

- components such as microchips used in electronics
- electronic assemblies
- integrated hardware and software devices such as network routers, laptops, and cellphones
- custom software systems and commercial software products

Computing System Supply Chain: Government



Government Supply Chain Risks

A key objective for Supply Chain Risk Management (SCRM) is to identify the aspects of a supply chain that are risks.

Management of commercial manufacturing supply chains typically focuses on availability risks: sufficient supply

Systems supply chain risks of interest are those that affect operations and can be instantiated by an active agent. Significant adverse events or threats include

- Inadvertent vulnerabilities created during development
- insertion of counterfeit components or product tampering during manufacture or delivery: Particularly for government systems

ICT SCRM Threats

Threats are events created attackers with malicious intent.

ICT SCRM Threats fall into two groups depending on where that malicious event occurs: malicious supply chain threats and malicious system threats. Malicious supply chain threats include

- A malicious event occurs somewhere along the supply chain.
  - the substitution of counterfeit item
  - tampering with an item during manufacture
- The attack exploited weaknesses in the management of the supply chain
- The outcome for these threats is that the acquirer does not receive an authentic item.

General Supply Chain Risks

Risk: The possibility that something unpleasant or unwelcome will happen (Oxford English Dictionary)

For a manufacturer, supply chain risks can include

- disruption of supply, inventory, and schedule (e.g., just-in-time inventory)
- changes in demand and customer preferences
- theft, counterfeiting
- confidentiality (e.g., Apple—product features)
- labor costs, exchange rates (e.g., Toyota)
- lack of human resources or capital
- changes in government policy or legislation

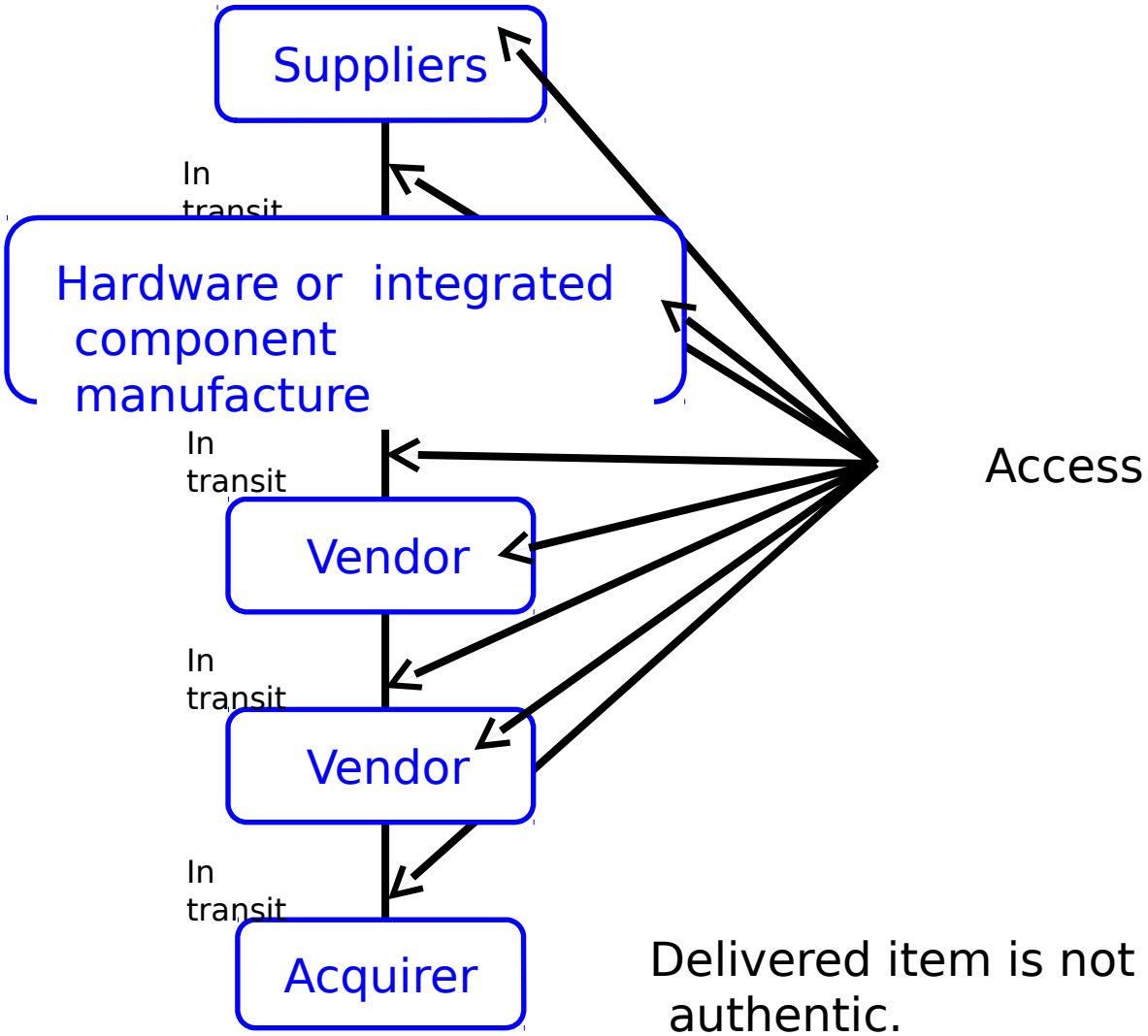
ICT Supply Chain Risks

Management of commercial manufacturing supply chains typically focuses on availability risks.

ICT supply chain risks of interest are those that affect operations and can be instantiated by an active agent (called the threat). Risks include

- intentional insertion of counterfeit components or product tampering during manufacture or delivery
- poor system development, integration, or operational practices that enable attackers to compromise a system
- system features that can be used to compromise a system

Malicious Supply Chain Threats



Counterfeit Individual Parts

Senate Committee on Armed Services Report United States Senate on May 21, 2012[1] provides examples of DoD counterfeit incidents.

- The committee identified 1800 cases of suspect counterfeit parts with the total number of items numbering over 1,000,000.
- These 1800 cases involved over 650 companies each with their own supply chains
  - More than 70 percent of the suspect parts are traced to China.
  - 80% of the supply chains started with a U.S supplier.
  - Complex supply chains mask the true origin of parts: In one case, the part had exchanged hands five times and went through four states and three countries after leaving the original supplier in China before it reached the subcontractor who built the hardware device.
  - Contractors were often not aware of the actual sources of electronic parts that were ordered.

Examples of Counterfeiting in DoD Supply Chains

The material on the current state of counterfeits in DoD supply chains is drawn from the report, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, published by, Committee on Armed Services, United States Senate on May 21, 2012[1].

- The committee identified 1800 DoD cases of suspect counterfeit parts with the total number of items numbering over 1,000,000.
- These 1800 cases involved over 650 companies each with their own supply chains
- An in-depth history is provided for four of the cases.
- A GAO report on on-line sales of counterfeit parts is included.

[1] http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

Senate Report on DoD Counterfeit Incidents

Sources

- The Committee tracked well over 100 of the approximately 1,800 cases of suspect counterfeit parts back through the supply chain.
- More than 70 percent of the suspect parts are traced to China.
- 80% of the supply chains started with a U.S supplier.
- Complex supply chains mask the true origin of parts.
  - In one case, the part had exchanged hands five times and went through four states and three countries after leaving the original supplier in China before it reached the subcontractor who built the hardware device.
  - Contractors were often not aware of the sources of electronic parts.

Instances of Counterfeit CISCO Routers

CISCO only sells through authorized suppliers

The lower prices have lead to government grey market purchases. The grey market refers to unauthorized sellers. The price is lower, but that lower price may be because the device is a counterfeit.

An authorized supplier could inadvertently supply a counterfeit. To meet a deadline, a supplier could have the router shipped by a third party who had the item in stock. The third party might not be an authorized supplier and substituted a low-cost

Example of ICT Counterfeit Risk

Government unit receives counterfeit CISCO routers.

Drop-shipped by third party who had it in stock

Used source with access to counterfeit products

Vendor

CISCO

Acquirer

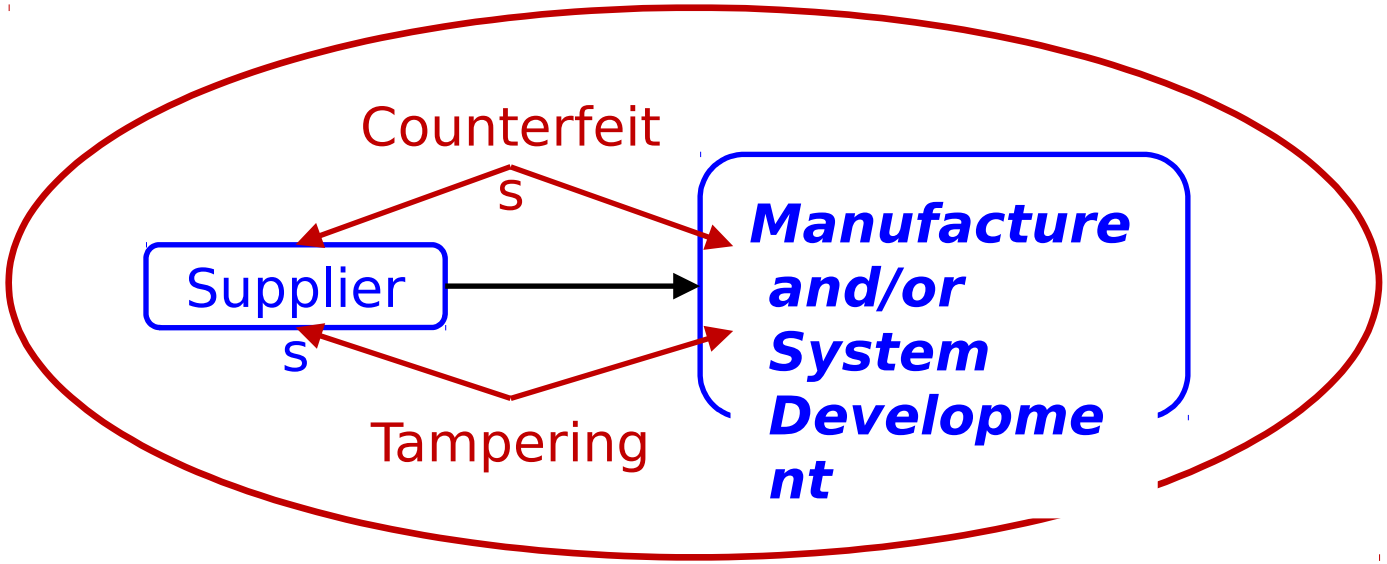
Did not purchase directly from manufacturer

Did not validate third-party supplier

“Upstream” Supply Chain Integrity

Counterfeit and tampering risks exist for a manufacturer’s supply chains, which are typically called “upstream” supply chains.

Selection criteria should include requirements for manufacturer SCRM practices for those upstream supply chains.



Hardware Electronics Threat Enablers: 1

The following threat enablers come from the Senate report.

Individual components

- In the DoD examples, many of the incidents were traced to intermediate distributors in the supply chain.
- Wide variation in testing for counterfeits
  - It is not enough to test how well a part functions. A part that passed a contractor's stress tests was later found to be a counterfeit after repeated failures of devices that contained it.
  - Testing for counterfeits requires exposing a part to aggressive solvents to determine whether markings are authentic or to breaking open part samples to examine the materials and method of construction.
  - In one instance, a sample of 18 parts were tested as part of a contractor's criteria for selecting a supplier, but no testing was done on the delivered items. The full order of 10,000 chips included counterfeits.

Hardware Electronics Threat Enablers: 2

Commercial electronic assemblies and commercial integrated products

- The suppliers for high-volume manufacturers are financially motivated to use strong supply chain controls by the risk of loosing the contract
- There can be higher risks of supply chain failures for suppliers to low-volume products.

Custom electronic assemblies and devices

- Contractors are not necessarily aware of the sources.
- Contractors often do not suffer a financial loss if counterfeits were found. The government pays for the repairs
- If the incidents are not maintained in a central repository, then other acquisitions will not aware of the problems with these specific suppliers or manufacturers.

Dynamics of Malicious Supply Chain Threats

In a Committee Staff interview, Raytheon's Vice-President of Supply Chain Operations noted

> *[W]hat keeps us up at night is the dynamic nature of this threat because by the time we've figured out how to test for these counterfeits, they've figured out how to get around it. And it's literally on almost a daily basis they change and the sophistication of the counterfeiting is amazing to us. We're finding that you have to go down to the microns to be able to figure out that it's actually a counterfeit.*

The sophistication of current counterfeiting techniques is likely beyond the in-house detection capabilities of most open-market suppliers.

Malicious Software System Threats – Attacker Objectives[1]

Malicious system threats target deployed systems with the objective to

- tamper with data – integrity
- disclose information – confidentiality
- deny access to a service – availability

A successful attack on a system frequently depends on

- spoofing an identity to gain illegal access
- an elevation of privilege is where an attacker gains additional access rights.
  - The attacker cannot log into a computer to run malicious software and instead incorporates it in a web page.
  - A user is persuaded to follow a link and unknowingly runs that software for the attacker when the browser loads that page.
  - The software runs using that user's access privileges, i.e. the attacker has gone from have no privileges to using that user's access rights.

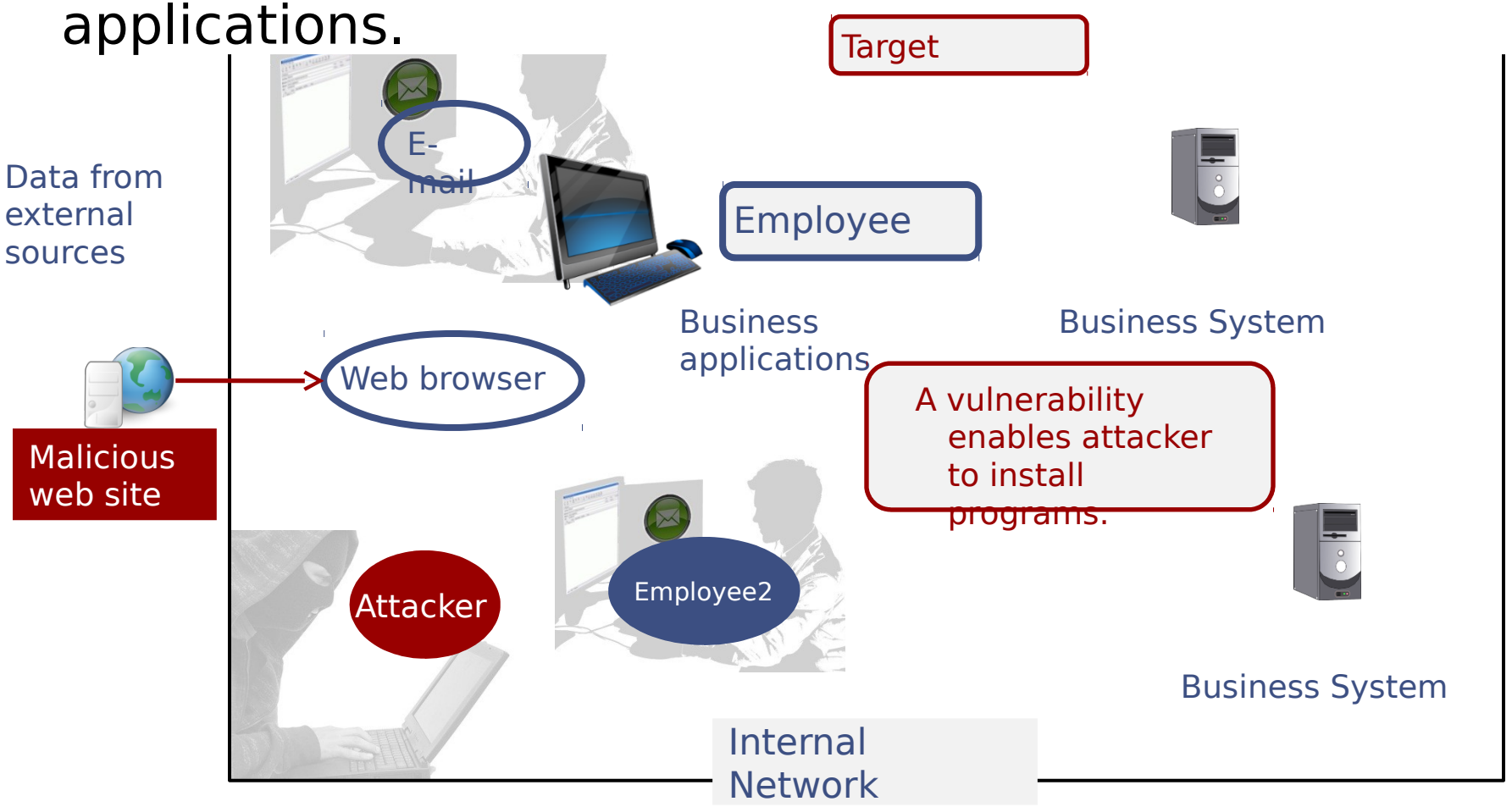
Acquisition Examples of Malicious System Threats

System requirements can create malicious system threats. For example cost, desired usage, or a near-term completion date can require use of commercial components with malicious system threats.

- Commercial off-the-shelf may not have been designed for the threats associated with critical government systems.
- Commercial software can have malicious system threats that are known only after a successful attack.
- Critical systems increasingly involve consumer-oriented products such as web browsers and cell phones.
  - For example, the features of a web browser that implement Gmail can also be used by an attacker to run malware.
  - We are only starting to learn about possible cell phone threats. The attack community has a definite advantage over developers.

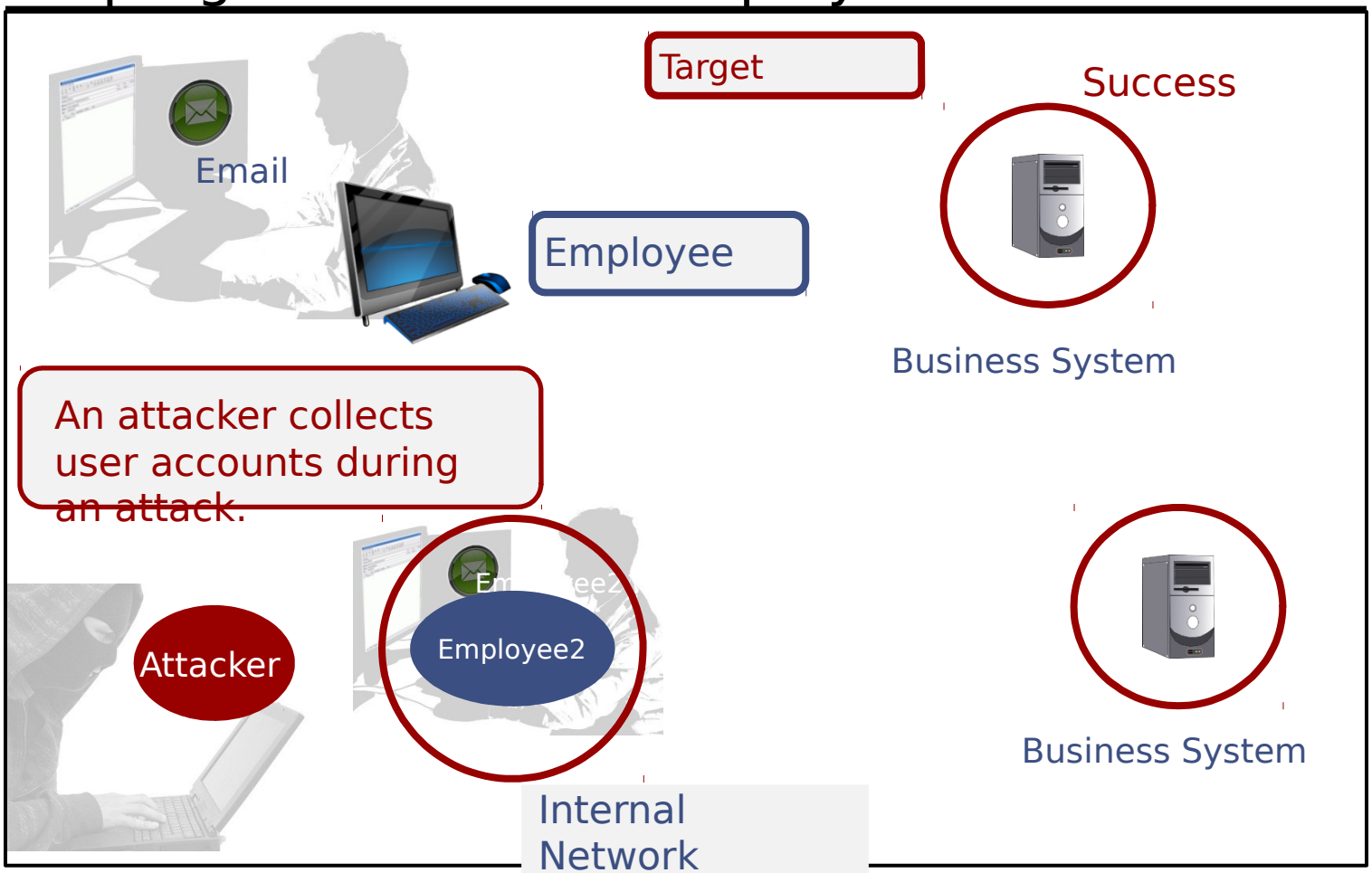
Attacks Exploit Weaknesses in Acquired Software

An organization's computing environment involves commercial and custom-developed software applications.



The Attacker Now Has the Advantage

An attacker has become an insider and can access the data and programs that the employee could.



Insecure Software

Long history of security vulnerabilities

- viruses on floppy disks
- network compromises
- operating systems
- software applications, as networks and operating systems become better secured

Mitigations: Widely accepted principles for developing secure software systems were published in 1975 but are rarely observed in practice.

- Principles assumed full knowledge of operational risks, whereas, in practice, systems are incrementally developed with incomplete knowledge.

State of Software Application Security

MITRE has documented over 700 software errors that have led to exploitable vulnerabilities: Common Weakness Enumeration (CWE).[1]

In 2010, 58% of all applications submitted to Veracode for testing did not achieve an acceptable security score upon first submission.[2]

Forrester Report: *Application Security: 2011 And Beyond* [3]

- 47% do not perform acceptance tests for third-party software.
- 46% follow homegrown application security methodologies instead of using ones that were independently validated.
- 27% do not perform security design.

1. http://cwe.mitre.org
2. http://www.veracode.com/content/view/1274/38
3. http://go.microsoft.com/?linkid=9777219

Consumer-Driven Adoption

There is a fundamental change in technology adoption.

The success of technologies such as the telegraph, telephone, networking, personal computers, and cellphones depended first on business adoption. Consumer usage followed later.

But the iPad, iPhone and Android cellphones are examples where consumer adoption is leading and often driving business adoption.

For example, the NSA has created a secure Android cellphone from commercially available components.

Tampering: Firmware

Every electronic device we pick up, a digital watch, a TV remote control, a mobile phone, an electronic hotel lock, or a DVD player includes software that adds functionality to the device. We refer to that software as firmware.

On a DVD or CD player such firmware ejects the media, reads the starting locations for the various media segments and implements the functions that repeat a selection or randomly play pieces.

Firmware is permanent in the sense that it is stored in read-only memory and often requires special updaters and physical access to the device to change it.

Firmware is a valuable target as an attacker can fundamentally change the operation of an electronic

Tampering with Software

We typically consider software vulnerabilities as accidental, i.e. not intentionally inserted during development.

Malicious tampering is a hardware supply chain risk, but the insertion of counterfeits is currently a more significant.

Firmware is software embedded in hardware devices. An attacker who can compromise the physical supply chain and access a device can also tamper with the firmware with significant consequences.

General SCRM Material

ELO 33.1.2

Given an acquisition scenario and supply chain requirements identify appropriate supply chain risk mitigations

SCRM Risk Assessments: NIST Special Publication 800-161

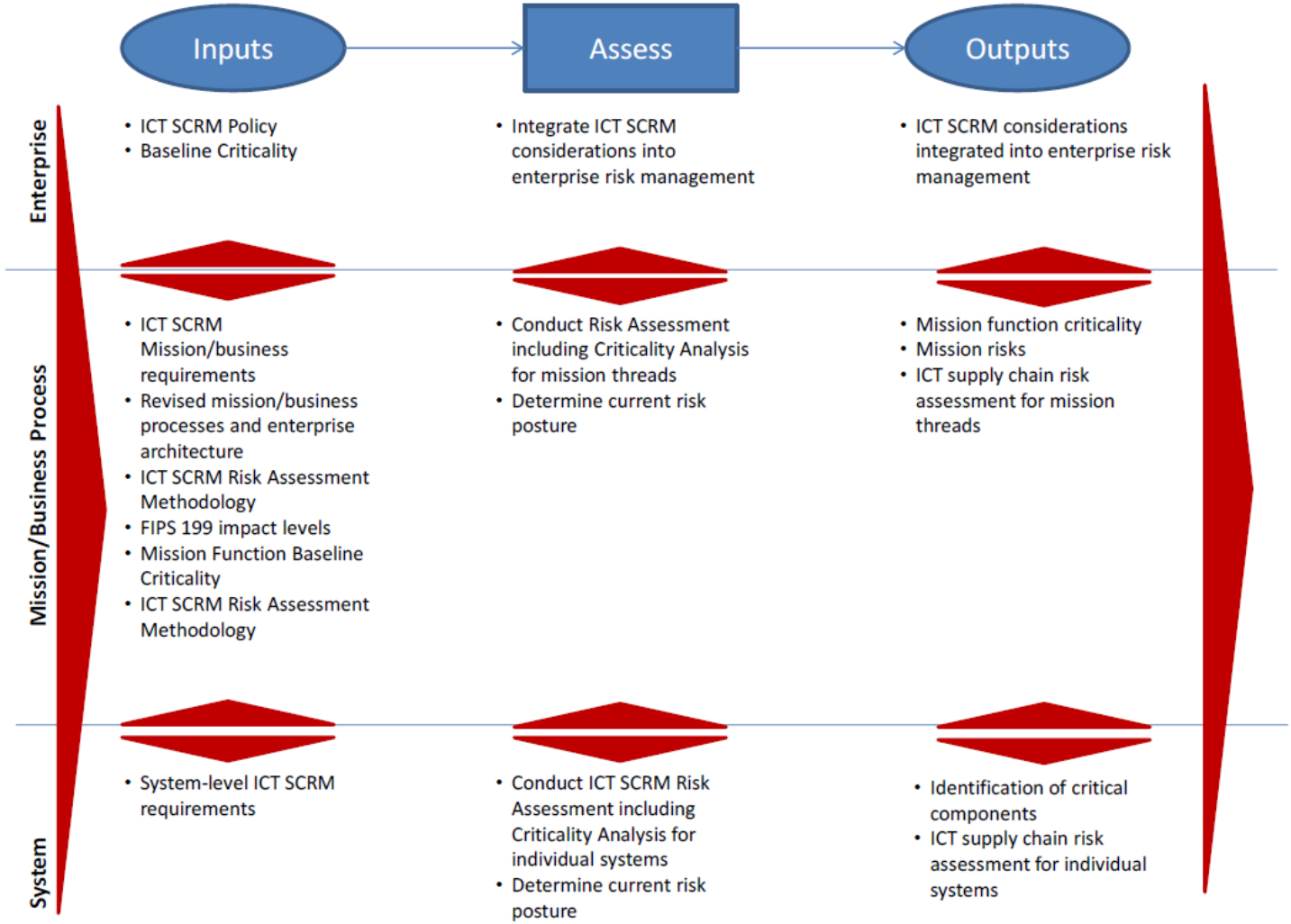

Inputs
Assess
Outputs
Enterprise
• ICT SCRM Policy
• Baseline Criticality
• Integrate ICT SCRM considerations into enterprise risk management
• ICT SCRM considerations integrated into enterprise risk management
Mission/Business Process
• ICT SCRM Mission/business requirements
• Revised mission/business processes and enterprise architecture
• ICT SCRM Risk Assessment Methodology
• FIPS 199 impact levels
• Mission Function Baseline Criticality
• ICT SCRM Risk Assessment Methodology
• Conduct Risk Assessment including Criticality Analysis for mission threads
• Determine current risk posture
• Mission function criticality
• Mission risks
• ICT supply chain risk assessment for mission threads
System
• System-level ICT SCRM requirements
• Conduct ICT SCRM Risk Assessment including Criticality Analysis for individual systems
• Determine current risk posture
• Identification of critical components
• ICT supply chain risk assessment for individual systems

Figure 2-6: ICT SCRM in the Assess Step

The Feasible and The Impossible

A characteristic of good supply chain risk management is an understanding what is feasible and cost effective.

Supply chain uncertainty is a given. We will never have complete product and supplier information.

Do not put the “impossible” on your critical path.

- Finding malicious code inserted by an expert trusted insider is beyond our current capabilities.
- It is very difficult to monitor participants in “long” supply chains.
- Expertly manufactured counterfeit products can be difficult to identify.

The objective of a cost-effective countermeasure might be to make attacks harder in terms of skills resources and effort required rather than prevent

Supply Chain Risk Management (SCRM) Acquirer Life Cycle Activities

SCRM planning

- be aware of potential threats in the supply chain that could impact the system during development and operations
- set supplier selection criteria to specify secure development capabilities
- monitor and verify that SCRM requirements are met

Manage the requirements that can increase supply chain risks.

- balance cost, security, functionality, operational usage

Manage the changes in supply chain risks

- during development
- after a system is deployed

Acquirer Risk Management Governance

No system is risk free.

Risks may have to be accepted to meet essential requirements.

Supply chain risks are shared among integrated systems.

Assume attacks partially succeed.

- monitor internal systems.
- plan for recovery.

Understand The Dynamics

As counterfeit and tampered product detection improves, the threat agents devise new techniques to slip by the test.

The same dynamics exist for the threats against systems that affect confidentiality, integrity, and availability. System sustainment contractors must also have threat identification and mitigation capabilities.

Attackers are normally a step ahead of the defenders.

- Total protection is not possible.
- A persistent and skilled attacker is likely to succeed..

Select Appropriate Mitigations

Risk: It is highly likely that a set of wire cutters used in a work area will be missing.

Threat: Workers forget to return them—effective

Threat: Passer-by steals them—not effective

Multiple Sources for Attack Enablers

Requirements: What We Want

- Some product features or usage can increase risks.
- Attackers are often ahead of developers in terms of knowing how leading-edge technologies or features can be compromised.

Design and Implementation: How We Do It

- For example, using externally developed products to reduce expense or development time can raise supply chain risks.

Tradeoffs

Supply chain risk analysis is a cost-benefit analysis based on the business impact of an exploit, the cost and effectiveness of mitigations, and the importance of requirements.

Mitigation decisions can involve

- system stakeholders
- acquisition professionals
- contractors: development and sustainment
- end users
- operational staff

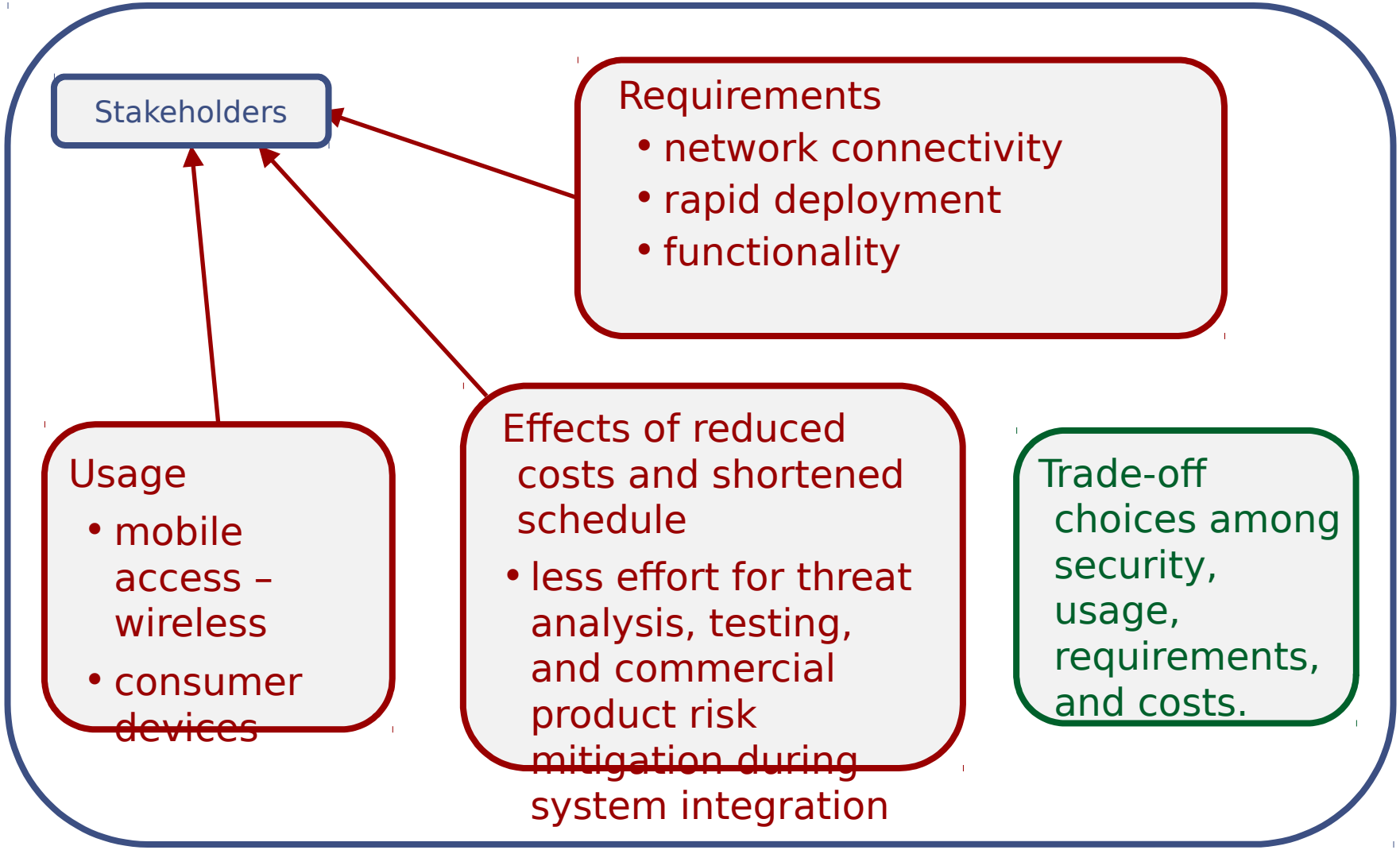
Malicious System Threats Can Lead to Requirement Changes

System requirements may need to be revised if risks associated with associated malicious system threats are not acceptable. That decision is depends on cost-benefit analysis based on the business impact of an exploit, the cost and effectiveness of mitigations, and the value of requirements.

Mitigation decisions can involve

- system stakeholders
- acquisition professionals
- contractors: development and sustainment
- end users
- operational staff

Stakeholder Risk Acceptance


Stakeholders
Requirements
• network connectivity
• rapid deployment
• functionality
Usage
• mobile access – wireless
• consumer devices
Effects of reduced costs and shortened schedule
• less effort for threat analysis, testing, and commercial product risk mitigation during system integration
Trade-off choices among security, usage, requirements, and costs.

Summary Possible Guidance

Counterfeits & tampering

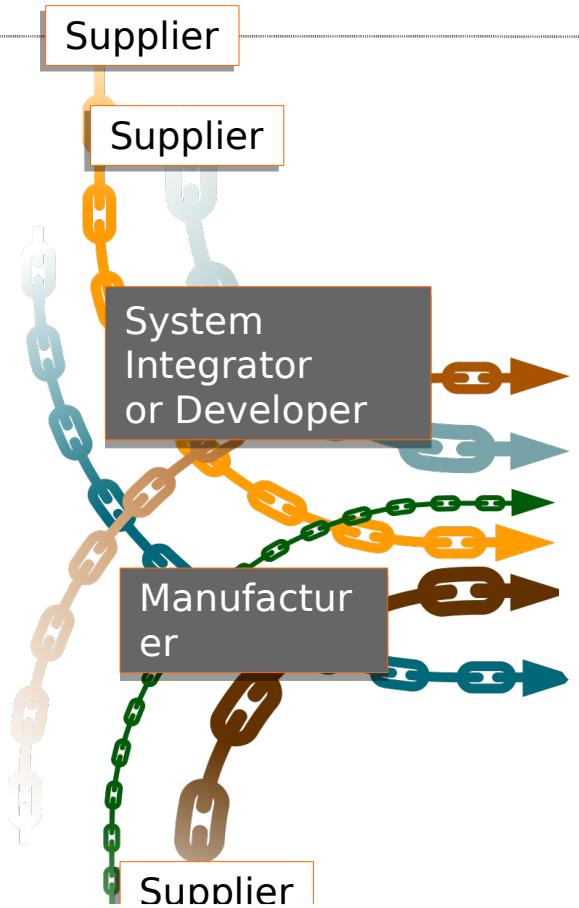
Supply chain attack

Insecure supply chain and untrustworthy suppliers

Acquisition practices to better secure supply chains and validate suppliers

SCRM requirements for suppliers

Verification that supplier's SCRM practices effectively applied



Long and complex international supply chains

Highly skilled and well financed adversaries

Deployed system compromised System attack

Unintentional system weaknesses

Development lifecycles that create secure software

Acquisition practices that identify suppliers with required capabilities

Verification that development practices effectively applied for acquired system

Supply Chain Integrity Practices

Primary hardware SCRM objective

- Address the security and proper execution of supply chain integrity practices that are applied to components during their sourcing, manufacture, development, and delivery and that reduce the risk of a supplier delivering compromised products to customers.

Scope

- Acquirer’s supply chain integrity practices—inspections and acceptance testing
- Supplier’s supply chain integrity practices—selection criteria

Evaluate Developer Capabilities for SCRM

Challenge: Evaluate a developer capabilities as part of a supplier selection.

- An assessment could consider
  1. supplier claims for the system development life cycle practices
     - Supplier claims may not be what is actually done.
  2. the specific practices used by suppliers
     - We should compare the results of practices rather than the practices. The choice of how to achieve a result varies widely among developers.
  3. evidence that the practices are widely applied
     - Some supplier's claims are applicable only to a subset of the efforts.
     - The Open Group's assessment of commercial-off-the-shelf suppliers and developers concentrates on this item.
     - There are opportunities to verify that practices are applied for contracted system development.
     - This can be monitored for contracted system development.

Hardware Mitigations

Hardware Supply Chain Mitigations

The primary risk is the delivery of a non-authentic unit. Such a unit might contain counterfeit components or be the target of tampering during manufacturing or delivery.

Supply chain integrity practices: The collection of processes and controls that reduce the risk of a supplier delivering a compromised product to customers

- Limit access to hardware while in transit or during manufacture.
- Use approved suppliers.

Countermeasures to Prevent a Compromised Supply Chain

What are the mitigations for threats that require physical access such as inserting counterfeits or tampering with hardware or firmware?

Supply chain integrity practices are the collection of processes and controls that reduce the risk of a supplier delivering a compromised product to customers. Examples include

- Limit access to hardware while in transit or during manufacture.
- Use approved suppliers.

Hence a supply chain SCRM objective is

- Address the security and proper execution of supply chain integrity practices that are applied to components during their sourcing, manufacture, development, and delivery and that reduce the risk of a supplier delivering compromised products to customers

Countermeasures: Counterfeit and Tampered Products: 1

To avoid the supply chain risks of multiple procurements for very critical chips, a single highly controlled procurement of a sufficient number to meet the needs for the full life of a device could be done.

A blind buy where knowledge of the usage and/or the specific purchaser is restricted can reduce risks.

Parts should be marked.

- The objective of such markers is not necessarily to eliminate the risk but to increase resources and expertise required by threat agents.

Require proper disposal of electronic equipment to avoid have retired equipment entering the supply chain for counterfeiters.

Countermeasures: Counterfeit and Tampered Products: 2

The services of specialized testing laboratories should be considered.

- Suppliers for the general market are not likely to have the expertise to identify counterfeits.
- Incorporate random inspections and testing of product samples into procurements. The acquiring agency should consider having or contracting for an independent testing capability.

Use approved suppliers

- Try to use short supply chains, i.e. with few intermediate distributors, for critical items.
- Counterfeit and tampering instances should be reported so that later acquisitions can avoid those suppliers.
- For critical items, require an auditable chain of custody from manufacturer to acquirer.
- Manufacturer's and supplier's practices should sufficiently

Software Risks and Mitigations

Change in Technology Adoption: Consumer-Driven

There is a fundamental change in technology adoption.

The success of technologies such as the telegraph, telephone, networking, personal computers, and cellphones depended first on business adoption. Consumer usage followed later.

But the iPad, iPhone and Android cellphones are examples where consumer adoption is leading and often driving business adoption.

For example, the NSA has created a secure Android cellphone from commercially available components.

Trend increases potential software supply chain risks.

- Time to market is often primary driver
- Limited attention to security

Difficulties

Supply chain uncertainty is a given. We will never have complete product and supplier information.

Hardware Supply Chains

- It is very difficult to identify counterfeit or tampered products. This risk cannot be eliminated.

Software Supply Chains

- Many of the mitigations involve improved software quality, which is a difficult, elusive, and often ambiguous objective.
- Continuing changes in threats, exploitable weaknesses, personnel, usage, and technology exist.
- An increasing number of enablers are associated with desired software features.
- A persistent and skilled attacker is likely to succeed.

External Controls Not Sufficient to Mitigate Software Process Threats

The increased likelihood of a rollover is a design weakness for sports utility vehicles.

Revised design

- Sensors recognized unstable conditions and software controls intervened
- Safety built into the design

Software weakness: poor handing of unexpected conditions such as not rejecting invalid input

Becomes a vulnerability when an attacker can create conditions that leads to adverse behavior.

- Installs a program
- Accesses or changes protected data

Development Risk Mitigation

Significant step forward in 2006 with the publication of Microsoft's *Security Development Lifecycle*[1]

- Security considered from the beginning of the software development life cycle.
- For example, a developer of software for database access considers how the software could be exploited during development.
- Practices are not new, but Microsoft documented how they could be applied to reduce the number of inadvertent vulnerabilities created during development.
- Microsoft's demonstrated success encouraged similar activity by other software development organizations.

1. http://www.microsoft.com/security/sdl/default.aspx

Survey of Security Initiatives

The success of Microsoft's security initiative that started in 2002 lead to the publication of the Security Development Lifecycle in 2006 encouraged the creation of security for a number of organizations.

BSIMM is the result of a multi-year study led by Cigital and Fortify. The study reviewed the efforts of sixty-seven large commercial organizations to improve security. The latest version, BSIMM-5, was released in the fall of 2013.

An analysis of the data collected by the surveys provides evidence that the success of a security initiative for a large organization depends on much more than security expertise.

Building Security In Maturity Model (BSIMM)-1

BSIMM only provides data – not a list of best practices

- Think of the BSIMM as being produced by *software engineering anthropologists* who catalog observed behaviors but with no judgments.
- The objective is to identify what is currently done rather than to promote specific practices.
- Widely-used practices are not necessarily best practices, but practices widely applied by organizations with good security records deserve further study.

Building Security In Maturity Model (BSIMM)-2

Survey identified 110 security processes that were organized into four groups and twelve practice areas

1. governance: policy & compliance (enforce effective application of development practices) strategy & metrics, training
2. knowledge (called Intelligence): attack models, proven security features and designs, applicable standards and requirements
3. software security development lifecycle activities (SSDL Touchpoints) architecture and design analysis, code review, security testing
4. deployment: vulnerability and configuration management, penetration testing, operational environment

Development Capabilities to Mitigate Software Threats

Strategic commitment to development of secure software:

organization governance

- training
- compliance and policy
- consistent and effective application - metrics
  - establish security checkpoints and milestones at various points in the development life cycle
  - require security sign-offs at various points in development

Expertise

- up to date attack and threat knowledge
- knowledge and use of appropriate standards – ISO 27034 application security

Development life cycle

- design analysis
- security testing

Validation and Verification

Validation and Verification of SCRM Mitigations

Validation

- What are the supply chain requirements that if met acceptably reduce supply chain risks?

Verification

- Does a specific supplier satisfy those requirements?

At this time, there is not a set of accepted requirements for SCRM.

Requirements based on applying specific practices have not been effective.

- There is significant diversity in the security practices applied by industry – see BSIMM survey.
- There are multiple ways to achieve the desired results.
- Rather than evaluating the process by which an engineering was made, we should evaluate our confidence in the predicted result based on the available information.

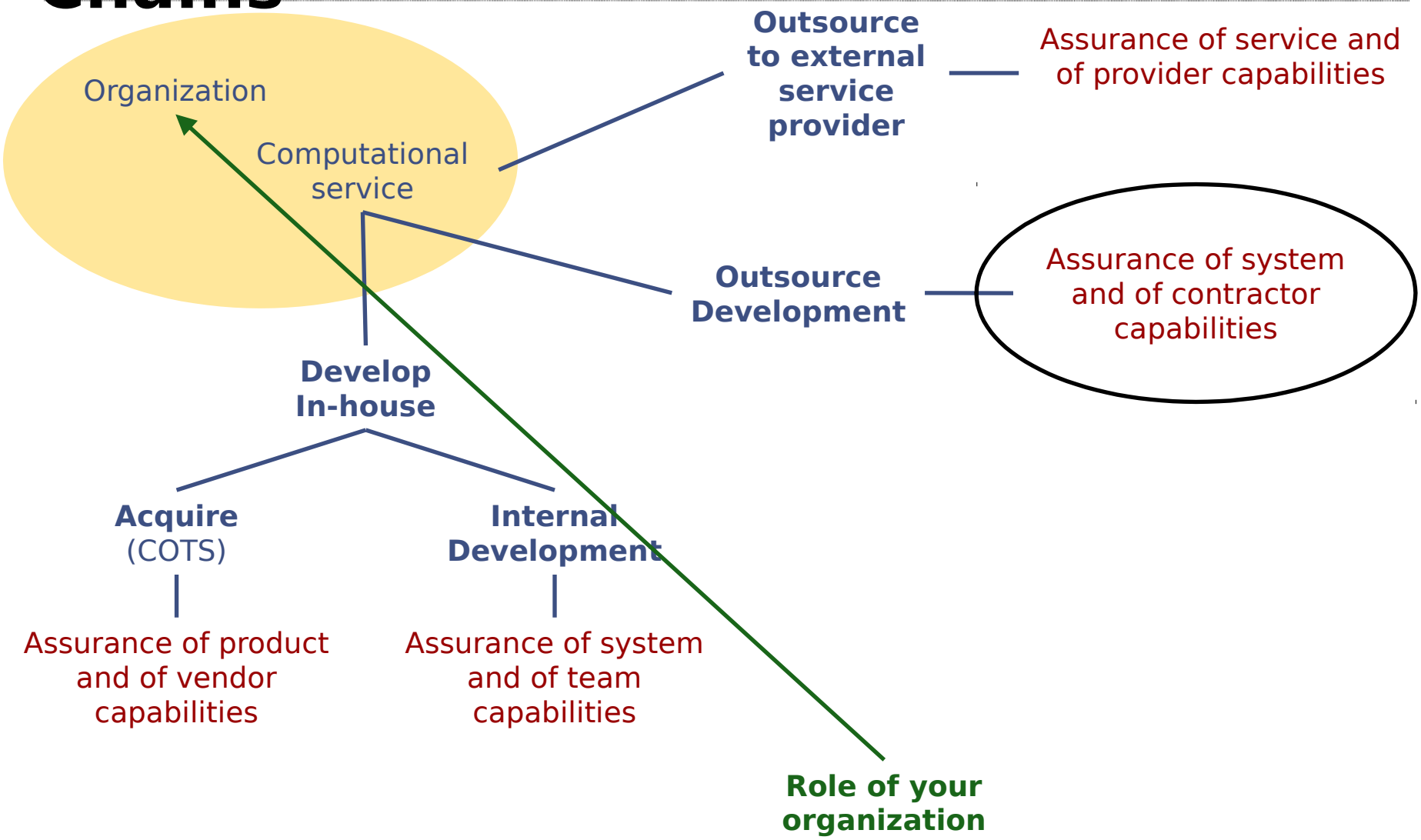
Verification

We need a way to evaluate supplier claims questions based on engineering analysis rather than just opinions.

For example, we might have a requirement that a supplier's employees are educated in security engineering practices.

How could suppliers support a claim that the requirement has been meet.

Showing Assurance For Supply Chains


Organization
Computational service
Outsource to external service provider
Assurance of service and of provider capabilities
Outsource Development
Assurance of system and of contractor capabilities
Develop In-house
Acquire (COTS)
Internal Development
Assurance of product and of vendor capabilities
Assurance of system and of team capabilities
Role of your organization

Evidence That Practices are effectively applied

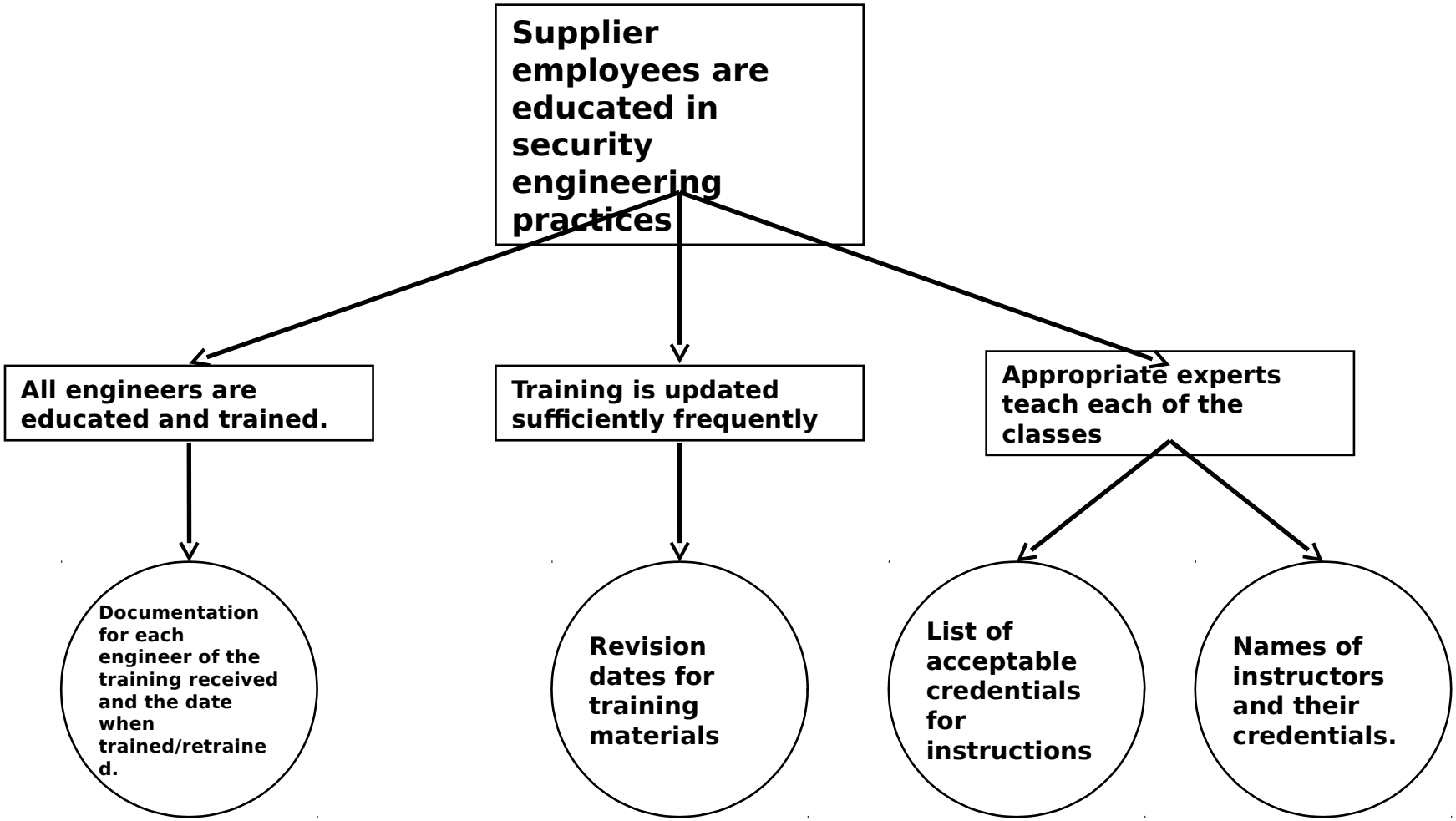
Software Engineering Institute (SEI) assessments have observed instances where the effectiveness for a specific practice ranged from 35% to 90%.

Measuring effectiveness is difficult to for risk focused development.

- Experts often disagree on threat priorities and choice of mitigations
- Threat analysis will always be incomplete.
  - complexity of a system supply chain – too many suppliers
  - changing nature of threat – new vulnerabilities and attack techniques
  - always limited by cost and schedules.

There will always be vulnerabilities and unknown threats, but the lack of attention to known threats only makes it easier to compromise systems.

An Assessment Requires an Assurance Argument and Evidence


Supplier employees are educated in security engineering practices
All engineers are educated and trained.
Training is updated sufficiently frequently
Appropriate experts teach each of the classes
Documentation for each engineer of the training received and the date when trained/retrained.
Revision dates for training materials
List of acceptable credentials for instructions
Names of instructors and their credentials.

Assurance

Assurance case: a documented body of evidence that provides a convincing and valid argument that a specified set of critical claims about a system's properties are adequately justified for a given application in a given environment.

An analysis of an assurance case does not evaluate the process by which an engineering decision was made. Rather it is a justification of a predicted result based on available information. An assurance case does not imply any kind of guarantee or certification. It is simply a way to document the rationale behind system design decisions.

Assurance: SQL Injection Vulnerability

A Standard Query Language (SQL) injection is usually near the top of a list of the most dangerous vulnerabilities.

It can occur when user input such as a “name” is used to construct a database command to retrieve data on that person. If the input is not verified a skilled attacker can submit database commands as part of that input that changes what is supposed to request for information into a construct changes or deletes database information.

Supply chain risk: It can be difficult to verify that a programmer-written routine prevents an SQL injection.

SQL Injection Risk Mitigation

We want to reduce or eliminate the risk of a SQL Injection before coding beings.

- Design analysis considers how the software could be compromised – often referred to as threat modeling.
- Incorporate a mitigation in the design.
- An assurance case justifies and provides evidence that mitigation has been effectively implemented.

CISQ Quality Rules

The Consortium for IT: Software Quality (CISQ) follows such an approach in developing specifications for automating the measurement of software reliability, security, performance efficiency, and maintainability

The CISQ assessment of the structural quality of software is based on applying rules of good coding practices (Quality Rules).

CISQ Quality Rules for security are based on MITRE's Common Weakness Enumeration, a list of over 900 weaknesses that have led to compromises.

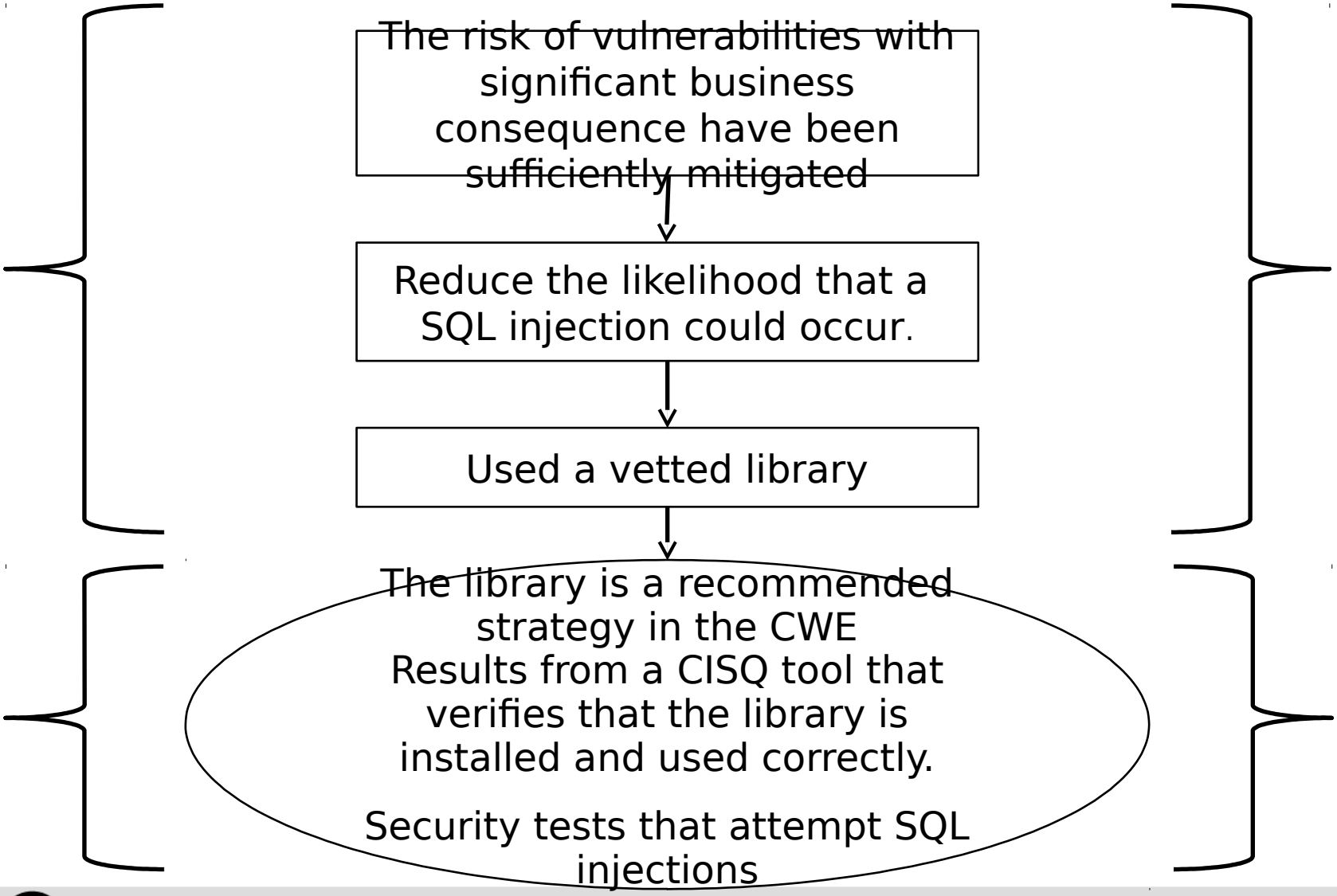
CAIS Rule 2

CWE-89: A SQL Injection

Quality Rule 2: Use a vetted library or framework that does not allow SQL injection to occur.

Quality Measure Element: Count the number of instances where user data that is used in a data query is not passed the vetted library. The desired value for this measure is zero, i.e. all such input data passes through the vetted library.

Assurance Case


The risk of vulnerabilities with significant business consequence have been sufficiently mitigated
Reduce the likelihood that a SQL injection could occur.
Used a vetted library
The library is a recommended strategy in the CWE
Results from a CISQ tool that verifies that the library is installed and used correctly.
Security tests that attempt SQL injections
Argu
nt
Evid
ce

Supply Chain Assessments

Can include

- Product risks: Internal development
  - product development/engineering method
  - secure development/engineering method
- System supply chains: Outsourced development
  - third-party hardware and software
  - outsourced development and manufacture

Internal Development

Product Development/Engineering Method

- well- defined, documented, and repeatable product development or engineering method and/or process
- effectiveness of the method is managed through metrics and management oversight.

Secure Development/Engineering Method

- software providers
  - employ methods or processes with the objective of identifying, detecting, fixing, and mitigating defects and vulnerabilities
  - verify the security and resiliency of the finished products.
- hardware providers
  - mitigate use of unverified and inauthentic software
  - protect against counterfeit hardware or software

Product Development: Open Group Evidence-based Examples

Threat Analysis and Mitigation

Vulnerability Analysis and Response

Secure Engineering Practices

Evolution of Development Practices

Threat Analysis and Mitigation-1

An assessor would like to find evidence that the developer has

- has identified a set of potential attacks and how they could be executed
- has described how those attacks could be best prevented or mitigated
- has assessed product architecture and design against potential attacks
- used the threat analysis to design test plans
  - evidence-based: test plans include
    - potential attacks patterns
    - likely occurring software weaknesses: example fuzz testing for inputs
    - mitigations and security controls incorporated in software

Threat Analysis and Mitigation-2

An assessor would like to find evidence such as

- documentation of architecture and design processes
- a list of known potential attacks.
- reports on threat assessments done against architecture and design
- reports on vulnerability analysis done during all phases
- process documentation for creation of test plans
- a sample of test plans and results

Vulnerability Analysis and Response

An assessor would like find evidence for

- techniques such code review, static analysis, penetration testing, white/black box testing are used for vulnerability analysis.
  - evidence-based
    - The attacks identified in the attack analysis are included in the vulnerability analysis: code scanning reports, code review reports
- vulnerability analysis and response feeds into the processes for ongoing product development, product patching, and remediation.

Secure Engineering Practices

An assessor would like to find evidence for

- secure coding practices such as input validation and use of appropriate compiler flags are used to avoid common coding errors – also in BSIMM
  - evidence-based
    - acceptable coding patterns, execution is shown from output from tools that enforce coding patterns, or from reports on manual code reviews

Evolution of Development Practices

An assessor would like to find evidence that

- changes to the threat landscape are monitored periodically.
- development/engineering practices, tools, and techniques are assessed and changed based on
  - changes in the threat landscape
  - the causal analysis of a new vulnerability in order to mitigate future occurrences

System Development: Lifecycle Checks

Business risks and attack surface analysis continues throughout life cycle. In particular such analysis should have guided top-level design decisions.

Security and assurance check points have been identified at various points in the life cycle

- Higher levels of assurance can require explicit measures at the check points and that exceptions are tracked.
- Such a requirement is supported by the 2011 version of the DoD Program Protection Plan and is a BSIMM Level 1 activity

Examples of Early Life Cycle Activities Checks

Have the security risks associated with system functionality (What we want) and with the proposed system implementation (How we build it) been identified?

- Developer knowledgeable of threats and attack enablers
- Developer is aware of the effects of system requirements and design decisions on security and mission threads (operations).

Examples of Middle Life Cycle Checks: 1

Are the appropriate standards and requirements in place for development

- There are security standards include those for secure coding.
- Security standards are shared with vendors and subcontractors.
- Do the vendors and subcontractors follow those standards?

What are the requirements for required security controls?

- Application input monitoring will be employed.
- The production software will be monitored for misbehavior and signs of attack.

Examples of Middle Life Cycle Checks: 2

Which failure conditions have the highest priority? How will those conditions be managed?

Have testing personnel participated in risk analysis and design work?

- Likely failure conditions have to be incorporated into the test plan.
- A software design requires bounds on the operating conditions. Testing should test those boundary conditions.

Examples of Late Life Cycle Activities Checks-1

What are the results of the code reviews?

Which system boundary conditions been tested.

- The tested conditions should include those that are likely to arise and affect mission success and those that could be exploited by an attack.
- High assurance could require that network protocols and system interfaces are subject to randomly generated faulty input – what is called fuzz testing. Fuzz testing is used by attackers to find vulnerabilities.
- Tests for high assurance could use adversarial knowledge to apply likely attack patterns.

Examples of Late Life Cycle Activities Checks-2

What kind of penetration testing is being done?

- Traditional penetration testing emulates an external attack.
- Penetration testing should be done with the assumption that an adversary has been able to achieve some kind of system access or is a “trusted” insider.
- Penetration testing for high assurance requirements should assume that the adversary is very knowledgeable about the system.

Open Group

The Open Group Trusted Technology Forum created the supply chain provider certification process for COTS suppliers.

The working groups members were employees of major COTS suppliers as well as some representation for US Federally Funded Research and Development Centers such as MITRE and the SEI.

COTS Assessment Constraints

Systems are increasingly developed by integrating COTS components

Assessment for COTS suppliers

- has to be low cost so smaller firms can afford it.
- can be adapted to hardware and software supply chains
- certification is for products but too expensive to assess individual products. Some suppliers have over 800 products
  - a certification is done for one or more products and should apply to all products developed with the same practices

Context

Motivations

- It is to the suppliers' advantage to only have to show that their development/manufacturing practices satisfy an accepted standard for a level of supply chain risk management practices
- The COTS developers/manufactures have development/manufacturing practices customized to specific products – changes in company development lifecycles not a viable option.
  - COTS suppliers must manage costs to remain competitive.
  - An assessment should verify the output of the practices, i.e. what was done and how well it was done and not how it was done.
  - Solution: evidence-based claims.

Open Group Example

The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of business.

Specific requirements:

SC_RSM.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.
SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.
SC_RSM.04	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be followed routinely.
SC_RSM.05	The mitigation plan should be reviewed periodically by practitioners, including management, and revised as appropriate.

Open Group: Accreditation

The certification process is implicitly analysis the assurance associated with an organization's COTS life cycle practices

- The standard provides subclaims in the form of guidelines, requirements, and recommendations.
- It suggests evidence that can demonstrate that subclaims have been satisfied.
  - "Implementation Selection Criteria Application (ISCA) Document" http://ottps-accred.opengroup.org/docs/O-TTPS_ISCA_Document.doc
- The subclaims and suggested evidence provide the means for an independent laboratory to do the analysis required to justify the certification.

Government regulations and supply chain requirements

For Government Systems

Common Criteria for Information Technology Security Evaluation (CC) Evaluation of security functions. Required of military systems. http://www.commoncriteriaportal.org/cc/

Supply Chain Risk Management Practices for Federal Information Systems and Organizations: NIST: http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf

US Government Documentation

Federal Information Security Management Act OMB Circular A-130, HSPD-12, FIPS Publication 200

FIPS 199: Standards for Security Categorization of Federal Information and Information Systems

FIPS 200: Minimum Security Requirements for Federal Information and Information Systems

OMB Circular A-130 : Management of Federal Information Resources

Federal Information Security Management Act (FISMA)

FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government.

Nine Steps

- Categorize the information to be protected.
- Select minimum baseline controls.
- Refine controls using a risk assessment procedure.
- Document the controls in the system security plan.
- Implement security controls in appropriate information systems.
- Assess the effectiveness of the security controls once they have been implemented.
- Determine agency-level risk to the mission or business case.
- Authorize the information system for processing.
- Monitor the security controls on a continuous basis.

Evaluate Security Functionality

Common Criteria for Information Technology Security Evaluation (CC) is a product assessment of its security properties.

- an international standard
- can be a requirement for non-government systems
- is a US Defense Department Requirement
- documents are available at http://www.commoncriteriaportal.org/cc/

Common Criteria

The CC permits comparability between the results of independent security evaluations by providing a common set of requirements

- for the security functionality of IT products
- for the assurance measures applied to these IT products during a security evaluation.

Independent laboratories are accredited to perform CC evaluations

Levels of Assurance-1

A protection profile is the set of security requirements.

CC defines 7 Evaluation Assurance Levels (EAL). For example

- EAL1: Functionally tested
  - some confidence in correct operation is required but the threats to security are not viewed as serious
- EAL2: Structurally tested
  - delivery of design information and test results,

Levels of Assurance-2

- EAL3 methodically tested and checked.
  - positive security engineering at the design stage without substantial alteration of existing sound development practices.
  - coverage of the implementation for a subset of security functionality
  - an architectural description of the design developed to understand the security behavior. .
  - selective independent confirmation of the developer test results
  - vulnerability analysis (based upon the functional specification) of the design.
  - security architecture description and guidance evidence provided.

Levels of Assurance-3

- EAL4 methodically designed, tested, and reviewed.
  - based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources.
  - additional design descriptions,
  - coverage of the implementation for the full set of security functionality.
  - improved mechanisms and/or procedures that increase the confidence that the product will not be tampered with during development.

Related Material-1

The SEI developed lectures for a course on assurance management. Four of those lectures cover aspects of SCRM. See http://www.cert.org/curricula/assurance-management.cfm

- AM-4-Intro-Assurance-Case.pttx
- AM-7-BSIMM.pttx
  - Survey of security practices done by large organizations
- AM-8-Assurrance-Case-OpenGroup.pttx
  - Detailed discussion of assurance and Open Group standard
- AM-9-Systems.pttx

Related Material-2

Software Assurance for Executives video modules and slide sets provide information and guidance on all stages of the software assurance lifecycle as well as emerging topics such as cloud computing and standards that support software assurance.

Software Assurance: Incorporate Security Early in Acquisitions

http://www.cert.org/curricula/software-assurance-for-execs.cfm

ELO 33.1.1.4

Given an acquisition scenario which lacks supply chain risk considerations, recommend acquisition requirements to effectively address supply chain risk.

ELO 33.1.1.5

ELO 33.1.1.5: Given a DoD IT acquisition scenario and associated SCRM plan, evaluate how it monitors and mitigates supply chain risks throughout the acquisition lifecycle.

Example: Using SCRM to Reduce Occurrence of Vulnerabilities

FAA 2009 objective: Create web site that provides current flight information obtained from an agency system to non-government organizations.

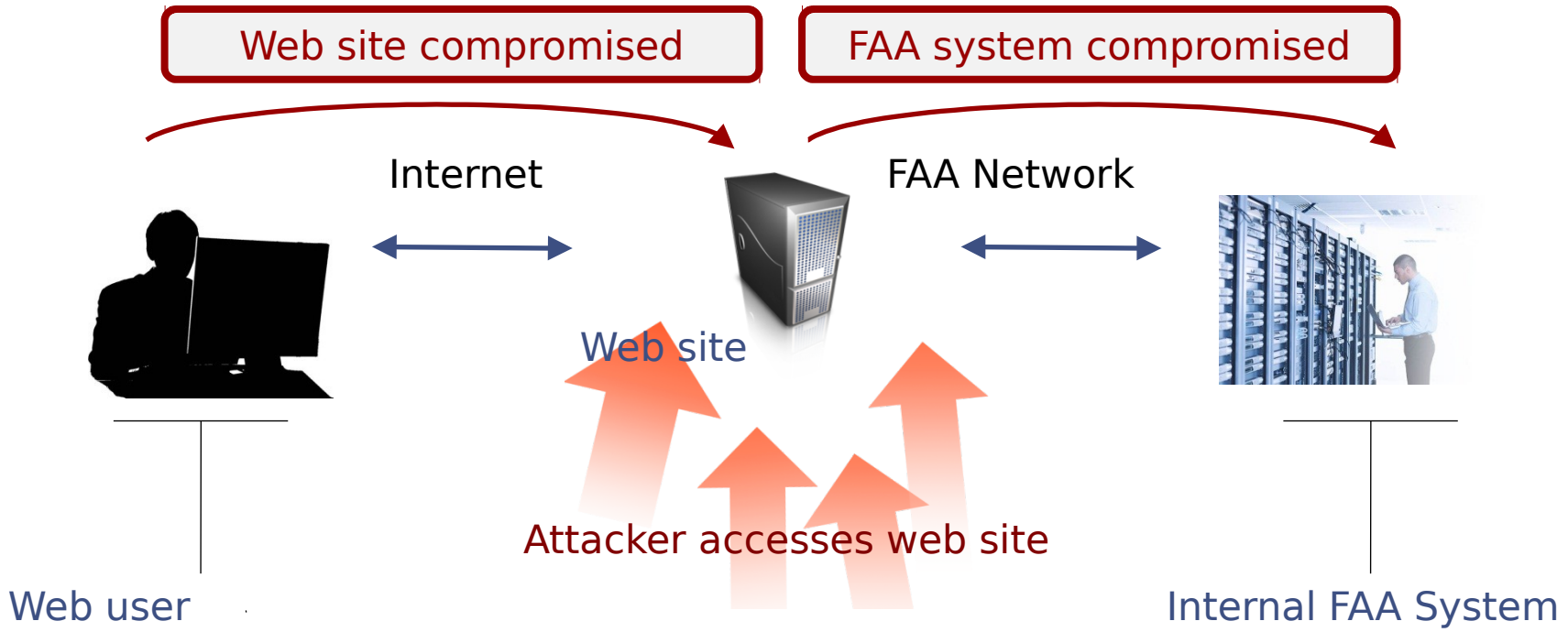
Acquirer should

- be aware of potential threats in the supply chain that could impact operations
- set supplier selection criteria to specify secure development capabilities
- monitor to verify that SCRM requirements are met

Acquirer SCRM: System Security Risks

Acquirer

- Are there specific security risks that should be addressed?



Acquirer Supplier Requirement: Consider Threats During Testing

Security testing capability includes applying known web attack patterns.

A team attempts to compromise web site from the Internet.

A team attempts to compromise FAA system from the web site.